

Polynomial Method in Tilings

Peter Horak¹ Dongryul Kim²

¹ School of Interdisciplinary Arts & Sciences

University of Washington, Tacoma, WA

e-mail: horak@uw.edu

² Harvard University, Cambridge, MA

e-mail: dkim04@college.harvard.edu

March 2, 2016

Abstract

In this paper we introduce a new algebraic method in tilings. Combining this method with Hilbert's Nullstellensatz we obtain a necessary condition for tiling n -space by translates of a cluster of cubes. Further, the polynomial method will enable us to show that if there exists a tiling of n -space by translates of a cluster V of prime size then there is a lattice tiling by V as well. Finally, we provide supporting evidence for a conjecture that each tiling by translates of a prime size cluster V is lattice if V generates n -space.

1 Introduction

A cluster in \mathbb{R}^n is the union of unit cubes centered at integer points with their sides parallel to coordinate axis; we note that a cluster does not have to be connected. This paper is devoted to tilings of \mathbb{R}^n by translates of a cluster.

An interest in tilings of \mathbb{R}^n by cubes goes back to a conjecture raised by Minkowski [11] in 1904; the conjecture stemmed from his work on geometry of numbers and quadratic forms.

Conjecture 1 (Minkowski). *Each lattice tiling of \mathbb{R}^n by cubes contains twins, a pair of cubes that share whole $n - 1$ dimensional face.*

Minkowski's conjecture was settled in the affirmative in 1941 by Hajós [3] who introduced in that paper a powerful algebraic method called “*splitting of groups*.” We note that although a cluster is a very special type of a tile, it provides a simplest known counterexample to part (b) of the 18th problem of Hilbert:

Problem 2. *If congruent copies of a polyhedron P tile \mathbb{R}^3 , is there a group of motions so that copies of P under this group tile \mathbb{R}^3 ?*

In other words, the second part of the problem asks whether there exists a polyhedron, which tiles 3-dimensional Euclidean space but does not admit an isohedral (tile-transitive) tiling. It is shown in [1] that there is a periodic tiling of \mathbb{R}^2 by a cluster depicted in Fig.1, but no isohedral tiling of \mathbb{R}^2 exists.

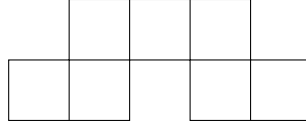


Fig.1.

In this paper we deal only with face-to-face (=regular) tilings of \mathbb{R}^n by a cluster C . It is not difficult to see that such a tilings can be seen as a tiling of \mathbb{Z}^n by translates of a subset V comprising centers of cubes in C . Thus, from now on, by a tile we will mean a set $V \subset \mathbb{Z}^n$. Throughout the paper we assume that $0 \in V$, and we deal exclusively with tilings \mathcal{T} of \mathbb{Z}^n by *translates* of V ; i.e.,

$$\mathcal{T} = \{V + l; l \in \mathcal{L}\}.$$

As $0 \in V$, we will identify each tile $V + l$ in \mathcal{T} with l . A tiling \mathcal{T} is termed periodic (lattice), if \mathcal{L} is periodic (lattice). Since \mathbb{Z}^n is a group, the fact that V tiles \mathbb{Z}^n can be expressed as

$$\mathbb{Z}^n = V + \mathcal{L},$$

meaning that each element of \mathbb{Z}^n can be written in a unique way as the sum of an element in V and an element of \mathcal{L} , and also as

$$|(-V + x) \cap \mathcal{L}| = 1$$

for each $x \in \mathbb{Z}^n$. In the area of tilings of \mathbb{Z}^n by translates of a set V most research is oriented towards solving several long-standing conjectures.

Conjecture 3 (Lagarias-Wang 1996, [10]). *If V tiles \mathbb{Z}^n , then V admits a periodic tiling.*

It is easy to see that the conjecture is true in the 1-dimensional case, but it is still open even for $n = 2$. It is known though that, for $n = 2$, the conjecture is true for polyominoes, cf. [1], i.e., if the corresponding cluster of cubes in \mathbb{R}^2 is connected. Moreover, Szegedy [14] proved the conjecture in the case when V is of a prime size. Further, Nivat [12] conjectured, that if V satisfies a complexity assumption, then each tiling of \mathbb{Z}^2 by V is periodic. We note that the famous Keller's conjecture [9] saying that each tiling of \mathbb{R}^n by cubes contains a pair of twin cubes was proved to be false for all $n \geq 8$, but it is still open for $n = 7$.

Our research has been motivated by two conjectures stated below. The first of them is likely the most famous conjecture in the area of error-correcting Lee codes:

Conjecture 4 (Golomb-Welch 1969, [2]). *The Lee sphere*

$$S_{n,r} = \{\mathbf{x} \in \mathbb{Z}^n : |x_1| + \cdots + |x_n| \leq r\}$$

does not tile \mathbb{Z}^n for $n \geq 3$ and $r \geq 2$.

Although there is a sizable literature on the topic, the conjecture is far from being solved.

The n -cross is a cluster in \mathbb{R}^n comprising $2n + 1$ cubes, a central one and its reflections in all faces. Thus, $\{0, \pm e_1, \dots, \pm e_n\}$ is the set of centers of cubes in the n -cross in \mathbb{Z}^n . It is known, see [5], that if $2n + 1$ is not a prime then there are uncountably many non-congruent tilings of \mathbb{Z}^n by the n -cross. It was conjectured there that:

Conjecture 5. *If $2n + 1$ is a prime then, up to a congruence, there is only one tiling of \mathbb{Z}^n by n -cross.*

We believe, if true, the conjecture goes against our intuition that says: The higher the dimension, the more freedom we get. The conjecture has been proved for $n = 2, 3$ in [5] and for $n = 5$ in [7]. Thus, there is a unique tiling of \mathbb{Z}^n by crosses for $n = 2, 3$, there are uncountably many tilings of \mathbb{Z}^4 by crosses, but in \mathbb{Z}^5 there is again a unique tiling by crosses.

To attack these two conjecture we first describe a new algebraic method, so-called “polynomial method” that will enable us to prove some general results on tiling \mathbb{Z}^n by translates of a cluster. We note that a similar method has been independently developed and used in [8], where the authors focus on Nivat’s conjecture. Szegedy [14] proved, using a new algebraic technique based on quasigroups, that if a tile V is of a prime size then each tiling of \mathbb{Z}^n by translates of V is periodic. The polynomial method provides a different proof of this result:

Theorem 6. *Let $V \subset \mathbb{Z}^n$, and \mathcal{T} be a tiling of \mathbb{Z}^n by translates of V . If $|V| = q$ is prime, then $q(\mathbf{v} - \mathbf{w})$ is a period of \mathcal{T} for any $\mathbf{v}, \mathbf{w} \in V$.*

Further, applying Hilbert Nullstellensatz, we provide a necessary condition for the existence of a tiling \mathbb{Z}^n by translates of a generic (arbitrary) set V . With this in hand we prove that if $V = \{0, v_1, \dots, v_{q-1}\}$ is of a prime size q and $\{v_1, \dots, v_{q-1}\}$ generate \mathbb{Z}^n then there is a tiling of \mathbb{Z}^n by translates of V if and only if there is a lattice tiling of \mathbb{Z}^n by V . We conjecture a much stronger result:

Conjecture 7. *Let $V = \{0, \mathbf{v}_1, \dots, \mathbf{v}_{q-1}\} \subset \mathbb{Z}^n$ of a prime size q tiles \mathbb{Z}^n by translates, and $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n . Then there is a unique tiling, up to a congruency, of \mathbb{Z}^n by V and this tiling is lattice.*

Clearly, if true, the above conjecture would imply Conjecture 5. To provide supporting evidence we prove the above conjecture for all primes ≤ 7 .

2 Polynomial Method

First we describe *Polynomial Method* that represents our main tool when tackling various tilings problems. Then we state results that, in our opinion, are of interest on their own, but also constitute an important ingredient in the proofs of main theorems of this paper.

Let $\mathcal{T} = \{V + l; l \in \mathcal{L}\}$ be a tiling of \mathbb{Z}^n by translates of V . We define a linear map $T_{\mathcal{T}} : \mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}] \rightarrow \mathbb{Z}$, where $\mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ is the commutative ring of Laurent polynomials generated by $x_1^{\pm 1}, \dots, x_n^{\pm 1}$, such that, for every $(a_1, \dots, a_n) \in \mathbb{Z}^n$,

$$T_{\mathcal{T}}(x_1^{a_1} \cdots x_n^{a_n}) = \begin{cases} 1 & \text{if } (a_1, \dots, a_n) \in \mathcal{L} \\ 0 & \text{otherwise.} \end{cases}$$

If the tiling \mathcal{T} will be clear from the context we will drop the subscript and write simply T . We note that T is uniquely determined as the monomials $x_1^{a_1} \cdots x_n^{a_n}$ form a basis of the ring. Let $Q_V \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a polynomial associated with V , where

$$Q_V(x_1, \dots, x_n) = \sum_{(a_1, \dots, a_n) \in (-V)} x_1^{a_1} \cdots x_n^{a_n}.$$

Then for any monomial $x_1^{m_1} \cdots x_n^{m_n}$,

$$\begin{aligned} T(x_1^{m_1} \cdots x_n^{m_n} Q_V) &= \sum_{(a_1, \dots, a_n) \in (-V)} |\{(a_1 + m_1, \dots, a_n + m_n)\} \cap \mathcal{L}| \\ &= |(-V + (m_1, \dots, m_n)) \cap \mathcal{L}| = 1. \end{aligned}$$

Since the map T is linear and any polynomial is a linear combination of monomials, we can immediately extend this equality to

$$T(PQ_V) = P(1, \dots, 1)$$

for any polynomial $P \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$.

In what follows we will present results on tilings of \mathbb{Z}^n by translates of a set $V \subset \mathbb{Z}^n$. Most of these results will be proved by utilizing properties of the linear map T and the polynomial Q_V . We have termed this approach *Polynomial Method*.

We start with a technical statement:

Theorem 8. *Let \mathcal{T} be a tiling of \mathbb{Z}^n by translates of V , and let a be an integer relatively prime to $|V|$. Then, for any polynomial $P \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$, we have*

$$T(PQ_V(x_1^a, \dots, x_n^a)) = P(1, \dots, 1).$$

Proof. This statement follows directly from the two lemmas given below since a can be represented as a product of primes not dividing $|V|$ and possibly -1 . \square

Lemma 9. *Let $p = 1$, or p be a prime which does not divide $|V|$. Then*

$$T(PQ_V(x_1^p, \dots, x_n^p)) = P(1, \dots, 1)$$

for any polynomial $P \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$.

Proof. Since the map T is linear, it is sufficient to prove that $T(MQ(x_1^p, \dots, x_n^p)) = 1$ for any monomial M . We have

$$\begin{aligned} T(MQ_V(x_1^p, \dots, x_n^p)) &\equiv T(MQ_V^p) = T(MQ_V^{p-1}Q_V) \\ &= (Q_V(1, \dots, 1))^{p-1} = |V|^{p-1} \equiv 1 \pmod{p} \end{aligned}$$

since $T(RQ_V) = R(1, \dots, 1)$ for any polynomial R . Thus $T(MQ_V(x_1^p, \dots, x_n^p)) \geq 1$ for all monomials M .

We also have

$$\begin{aligned} T(MQ_V(x_1^p, \dots, x_n^p)Q_V) &= \sum_{\mathbf{v} \in V} T(M \cdot x_1^{v_1} \cdots x_n^{v_n} \cdot Q_V(x_1^p, \dots, x_n^p)) \\ &\geq \sum_{\mathbf{v} \in V} 1 = |V| \end{aligned} \tag{1}$$

while on the other hand,

$$T(MQ_V(x_1^p, \dots, x_n^p)Q_V) = Q_V(1^p, \dots, 1^p) = |V|.$$

It follows that the equality holds for every term in (1). For some fixed $\mathbf{v} \in V$, we have $T(M \cdot x_1^{v_1} \cdots x_n^{v_n} \cdot Q_V(x_1^p, \dots, x_n^p)) = 1$ for every monomial M . Therefore $T(MQ_V(x_1^p, \dots, x_n^p)) = 1$ for every monomial M . \square

Lemma 10.

$$T(PQ_V(x_1^{-1}, \dots, x_n^{-1})) = P(1, \dots, 1)$$

for any polynomial $P \in \mathbb{Z}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$.

Proof. Again, it is sufficient to prove it for monomials. We first prove

$$T(MQ_V(x_1^{-1}, \dots, x_n^{-1})) \leq 1$$

for any monomial M . Suppose that

$$T(Mx_1^{-v_1} \cdots x_n^{-v_n}) = T(Mx_1^{-u_1} \cdots x_n^{-u_n}) = 1$$

for some distinct $\mathbf{v}, \mathbf{u} \in (-V)$. Then letting $M' = Mx_1^{-v_1-u_1} \cdots x_n^{-v_n-u_n}$, we get

$$T(M'Q_V) \geq T(M'x_1^{v_1} \cdots x_n^{v_n}) + T(M'x_1^{u_1} \cdots x_n^{u_n}) = 2$$

which contradicts the original property of Q_V . Thus $T(MQ_V(x_1^{-1}, \dots, x_n^{-1})) \leq 1$ for all M .

Consider $MQ_V(x_1^{-1}, \dots, x_n^{-1})Q_V$. Because $T(MQ_V(x_1^{-1}, \dots, x_n^{-1})Q_V) = Q_V(1, \dots, 1) = |V|$ and

$$T(MQ_V(x_1^{-1}, \dots, x_n^{-1})Q_V) \leq \sum_{\mathbf{v} \in V} 1 = |V|,$$

all terms must attain equality. It follows that $T(MQ_V(x_1^{-1}, \dots, x_n^{-1})) = 1$ for any monomial M . \square

Corollary 11. *Let $\mathcal{T} = \{V + l; l \in \mathcal{L}\}$ be a tiling of \mathbb{Z}^n by translates of V , and let a be an integer relatively prime to $|V|$ or $a = -1$. Then $\mathcal{T}_a = \{aV + l; l \in \mathcal{L}\}$ is a tiling of \mathbb{Z}^n by translates of a "blow-up" tile $aV = \{av; v \in V\}$.*

Proof. Set $S = aV$. Then

$$Q_S(x_1, \dots, x_n) = \sum_{(v_1, \dots, v_n) \in (-V)} x_1^{av_1} \cdots x_n^{av_n} = Q_V(x_1^a, \dots, x_n^a).$$

By the above theorem,

$$T(MQ_S) = T(MQ_V(x_1^a, \dots, x_n^a)) = M(1, \dots, 1) = 1$$

for any monomial M . Thus, for any $x \in \mathbb{Z}^n$,

$$|(-S + x) \cap \mathcal{L}| = 1,$$

that is, $\mathcal{T}_a = \{aV + l; l \in \mathcal{L}\}$ is a tiling of \mathbb{Z}^n by translates of aV . \square

The following corollary can be found in [14]. We provide here a short proof of this result.

Corollary 12. *Let $\mathcal{T} = \{V + l; l \in \mathcal{L}\}$ be a tiling of \mathbb{Z}^n by translates of V , and let a be an integer relatively prime to $|V|$. Then $l + a(v - w) \notin \mathcal{L}$ for each $l \in \mathcal{L}$ and $v, w \in V$.*

Proof. By Corollary 11, $\mathcal{T}_a = \{aV + l; l \in \mathcal{L}\}$ is a tiling of \mathbb{Z}^n by translates of aV , hence $\mathbb{Z}^n = aV + \mathcal{L}$. Assume that $l + a(v - w) \in \mathcal{L}$. Then

$$\begin{aligned} l + av &= aw + [l + a(v - w)] \quad \text{but also} \\ l + av &= av + l; \end{aligned}$$

that is, $l + av \in \mathbb{Z}^n$ would be covered by two distinct tiles of \mathcal{T}_a . \square

3 A Necessary Condition for the Existence of a Tiling

The main goal of this section is to present a necessary condition for the existence of a tiling of \mathbb{Z}^n by translates of a generic (arbitrary) tile V . To the best of our knowledge this is the first condition of its type. We start by recalling a famous theorem of Hilbert [4] that will be applied in the proof of this condition.

Theorem 13 (Nullstellensatz). *Let J be an ideal in $\mathbb{C}[x_1, \dots, x_n]$, and $S \subset \mathbb{C}^n$. Denote by $\mathcal{V}(J)$ the set of all common zeros of polynomials in J , and by $\mathcal{I}(S)$ the set of all polynomials in $\mathbb{C}[x_1, \dots, x_n]$ that vanish at all elements of S . Then*

$$\mathcal{I}(\mathcal{V}(J)) = \sqrt{J} = \{f \in \mathbb{C}[x_1, \dots, x_n] : f^n \in J \text{ for some } n \geq 1\}.$$

The following statement is the main theorem of this section.

Theorem 14. *Let $V \subset \mathbb{Z}^n$ be a tile. Then there is a tiling of \mathbb{Z}^n by translates of V only if there exist $(x_1, \dots, x_n) \in (\mathbb{C} \setminus \{0\})^n$ such that $Q_V(x_1^a, \dots, x_n^a) = 0$ simultaneously for all a relatively prime to $|V|$.*

Proof. To prove the theorem we show that if there is no $(x_1, \dots, x_n) \in (\mathbb{C} \setminus \{0\})^n$ such that $Q_V(x_1^a, \dots, x_n^a) = 0$ simultaneously for all a relatively prime to $|V|$ then there is no tiling of \mathbb{Z}^n by translates of V .

We start with an auxiliary statement:

(*) Let $\{f_i\}_{i \in I} \subset \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ be a set of Laurent polynomials such that there exists no $(x_1, \dots, x_n) \in (\mathbb{C} \setminus \{0\})^n$ with $f_i(x_1, \dots, x_n) = 0$ simultaneously for $i \in I$. Then there exist Laurent polynomials p_1, \dots, p_k and indices $i_1, \dots, i_k \in I$ such that

$$f_{i_1} p_1 + \dots + f_{i_k} p_k = 1.$$

Indeed, for each $i \in I$, consider a sufficiently large integer n_i which makes $(x_1 \cdots x_n)^{n_i-1} f_i \in \mathbb{C}[x_1, \dots, x_n]$; if $f_i \in \mathbb{C}[x_1, \dots, x_n]$, then we simply set $g_i = (x_1 \cdots x_n)^1 f_i$. Then $g_i = (x_1 \cdots x_n)^{n_i} f_i$ is not only a polynomial, but also a multiple of $x_1 \cdots x_n$. Consider the ideal $J \subset \mathbb{C}[x_1, \dots, x_n]$ generated by the polynomials g_i . By the condition, there is no $x \in (\mathbb{C} \setminus \{0\})^n$ that makes $g_i(x) = 0$ for all $i \in I$. On the other hand, $g_i(x) = 0$ if any one of x_1, \dots, x_n is zero since the polynomial is a multiple of $x_1 \cdots x_n$. Thus it follows that

$$\mathcal{V}(J) = \{(x_1, \dots, x_n) \in \mathbb{C}^n : x_1 x_2 \cdots x_n = 0\}$$

and therefore, by Hilbert's Nullstellensatz, $x_1 \cdots x_n \in \mathcal{I}(\mathcal{V}(J)) = \sqrt{J}$; i.e., there exists a positive integer m for which $(x_1 \cdots x_n)^m \in J$.

Let q_1, \dots, q_k and i_1, \dots, i_k be the polynomials and indices which make

$$\begin{aligned} (x_1 \cdots x_n)^m &= g_{i_1} q_1 + \dots + g_{i_k} q_k \\ &= (x_1 \cdots x_n)^{n_{i_1}} f_{i_1} q_1 + \dots + (x_1 \cdots x_n)^{n_{i_k}} f_{i_k} q_k. \end{aligned}$$

Then dividing both sides by $(x_1 \cdots x_n)^m$, we get

$$1 = f_{i_1} \frac{q_1}{(x_1 \cdots x_n)^{m-n_{i_1}}} + \cdots + f_{i_k} \frac{q_k}{(x_1 \cdots x_n)^{m-n_{i_k}}}.$$

The proof of (*) is complete.

We are ready to prove the theorem. Assume that there is no $(x_1, \dots, x_n) \in (\mathbb{C} \setminus \{0\})^n$ such that $Q_V(x_1^a, \dots, x_n^a) = 0$ simultaneously for all a relatively prime to $|V|$. By (*), we obtain Laurent polynomials P_1, \dots, P_t and integers a_1, \dots, a_t relatively prime with $|V|$ for which

$$P_1 Q(x_1^{a_1}, \dots, x_n^{a_1}) + \cdots + P_t Q(x_1^{a_t}, \dots, x_n^{a_t}) = 1. \quad (2)$$

Replacing all x_1, \dots, x_n with 1, we get

$$P_1(1, \dots, 1) + \cdots + P_t(1, \dots, 1) = 1/|V|. \quad (3)$$

Suppose that there exists a tiling of \mathbb{Z}^n by translates of V . By (2), we have, for any monomial M ,

$$\begin{aligned} T(M) &= T(M(P_1 Q(x_1^{a_1}, \dots, x_n^{a_1}) + \cdots + P_t Q(x_1^{a_t}, \dots, x_n^{a_t}))) \\ &= T(M P_1 Q(x_1^{a_1}, \dots, x_n^{a_1})) + \cdots + T(M P_t Q(x_1^{a_t}, \dots, x_n^{a_t})) \\ &= P_1(1, \dots, 1) + \cdots + P_t(1, \dots, 1) = 1/|V|, \quad (\text{by Theorem 8}) \end{aligned}$$

with respect to (3). Because this differs from 0 and 1, we arrive at a contradiction. \square

Remark 15. To demonstrate that the above condition is only a necessary one, consider a tile V given in Fig.2. We have $Q_V(x, y) = 1 + x + y + x^2 y$, and $x = 1, y = -1$ is a common root of $Q_V(x, y)$ and of $Q_V(x^3, y^3)$. That is, there is a non-zero common root of $Q_V(x^a, y^a)$ for each a relatively prime to 4, although there is no tiling of \mathbb{Z}^2 by V . However, we will prove in the next section that this condition is a necessary and sufficient condition for tiles of a prime size.

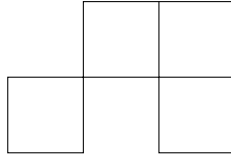


Fig.2.

One of the main strength of the above theorem is that it is not limited by a special size or by a special shape of the tile. On the other hand, it is very difficult to see whether the system has a common root if the size of the tile is composite. Therefore, it will require additional research to enable one to apply this theorem toward the Golomb-Welch conjecture. On the other hand, this theorem enables us to prove, see the next section, that there is a tiling of \mathbb{Z}^n by translates of a prime size tile V if and only if there is a lattice tiling by V .

4 Tiles of a Prime Size

Using Polynomial Method, we show that if V is a tile of a prime size then each tiling of \mathbb{Z}^n by translates of V is periodic, and that the existence of a tiling of \mathbb{Z}^n by V guarantees the existence of a lattice tiling.

Theorem 16. *Let $V \subset \mathbb{Z}^n$ be a tile, and \mathcal{T} be a tiling of \mathbb{Z}^n by translates of V . If $|V| = q$ is prime, then $q(\mathbf{v} - \mathbf{w})$ is a period of \mathcal{T} for any $\mathbf{v}, \mathbf{w} \in V$.*

Remark 17. *As mentioned in the introduction, Szegedy [14] proved the statement by using a new technique based on loops. Another proof of the above statement, using similar ideas, can be found in [8].*

Proof. Consider any monomial M . We have

$$\begin{aligned} T(MQ_V(x_1^q, \dots, x_n^q)) &\equiv T(MQ_V^q) = T(MQ_V^{q-1}Q_V) \\ &= (Q_V(1, \dots, 1))^{q-1} = q^{q-1} \equiv 0 \pmod{q} \end{aligned}$$

since $T(RQ_V) = R(1, \dots, 1)$ for any polynomial R . On the other hand, by definition

$$T(MQ_V(x_1^q, \dots, x_n^q)) = \sum_{(a_1, \dots, a_n) \in (V)} T(Mx_1^{-qa_1} \dots x_n^{-qa_n}).$$

Since the sum of $|V| = q$ terms, each of which are either 0 or 1, is a multiple of q , we conclude that every term must be either simultaneously 0 or simultaneously 1. Hence for any $\mathbf{v} = (v_1, \dots, v_n)$ and $\mathbf{w} = (w_1, \dots, w_n)$ in V ,

$$T(Mx_1^{-qv_1} \dots x_n^{-qv_n}) = T(Mx_1^{-qw_1} \dots x_n^{-qw_n}) = 0 \text{ or } 1.$$

It follows that for any $\mathbf{x} \in \mathbb{Z}^n$, the point \mathbf{x} is in \mathcal{L} if and only if $\mathbf{x} + q(\mathbf{v} - \mathbf{w})$ is in \mathcal{L} . Therefore $q(\mathbf{v} - \mathbf{w})$ is a period of \mathcal{T} . \square

To prove a main result of this section we first state a necessary and sufficient condition, in terms of a homomorphism, for the existence of a *lattice* tiling of \mathbb{Z}^n by translates of V . We will use this condition in the proof of the following theorem.

Theorem 18 ([6]). *Let V be a subset of \mathbb{Z}^n . Then there is a lattice tiling \mathcal{T} of \mathbb{Z}^n by V if and only if there is an Abelian group G of order $|V|$ and a homomorphism $\phi : \mathbb{Z}^n \rightarrow G$ so that the restriction of ϕ to V is a bijection.*

Now we are ready to show that the existence of a tiling guarantees the existence of a lattice one. We point out that the same statement in the language of Abelian groups, is given, with only a hint on the proof, in [14].

Theorem 19. *Let $V = \{0, v_1, \dots, v_{q-1}\} \subset \mathbb{Z}^n$ be a prime size tile, and suppose that $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n . Then there exists a tiling of \mathbb{Z}^n by translates of V if and only if there is a lattice tiling of \mathbb{Z}^n by translates of V .*

Proof. We assume that there exists a tiling and prove that there exists a lattice tiling. From Theorem 14, we see that there exists a common nonzero solution to $Q_V(x_1^a, \dots, x_n^a) = 0$, where a ranges over all integers not divisible by q . Let the terms of Q_V be the monomials m_1, \dots, m_q , where $m_1 = 1$. If $(x_1, \dots, x_n) \in \mathbb{C}^n$ is a common root, then for the corresponding values of $m_1, \dots, m_q \in \mathbb{C}$, we have

$$m_1^a + \dots + m_q^a = 0$$

for all $a = 1, 2, \dots, q-1$.

Because it can be inductively deduced that the elementary symmetric polynomials

$$\sum_{i_1 < \dots < i_t} m_{i_1} \dots m_{i_t} = 0$$

for $1 \leq t < q$, we get that $m_1, \dots, m_q \in \mathbb{C}$ are roots of a polynomial which is of the form

$$(X - m_1) \dots (X - m_q) = \sum_{t=0}^q (-1)^t X^{q-t} \sum_{i_1 < \dots < i_t} m_{i_1} \dots m_{i_t} = X^q - c.$$

Because $m_1 = 1$, the constant is $c = 1$, and thus m_1, \dots, m_q is a permutation of $1, \zeta, \dots, \zeta^{q-1}$ where $\zeta = e^{2\pi i/q}$.

Note that since $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n , each of x_1, \dots, x_n can be represented as a product of powers of m_1, \dots, m_q . This implies that the values $x_1, \dots, x_n \in \mathbb{C}$ are also powers of ζ . Let $x_i = \zeta^{a_i}$ for each i . From the fact that the values of $m_1, \dots, m_q \in \mathbb{C}$ is a permutation of $1, \zeta, \dots, \zeta^{q-1}$, it follows that the restriction of the homomorphism $\phi : \mathbb{Z}^n \rightarrow \mathbb{Z}/q\mathbb{Z}$ defined by

$$(k_1, \dots, k_n) \mapsto a_1 k_1 + \dots + a_n k_n$$

restricted to V is a bijection. Applying Theorem 18 finishes the proof. \square

5 A Conjecture on Lattice Tilings

It was proved in the previous section that the existence of a tiling of \mathbb{Z}^n by a prime size tile V guarantees the existence of a lattice tiling of \mathbb{Z}^n . In this section we focus on with Conjecture 7 which claims that a much stronger statement is true.

Conjecture 20. *If $V = \{0, v_1, \dots, v_{q-1}\} \subset \mathbb{Z}^n$ is of a prime size q and $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n then each tiling of \mathbb{Z}^n by V is a lattice tiling.*

The following example exhibits that the condition: “ $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generates \mathbb{Z}^n ” cannot be replaced by a weaker assumption that V is an n -dimensional tile.

Example 21. If $V = \{\mathbf{0}, \mathbf{e}_1, \dots, \mathbf{e}_{q-2}, 2\mathbf{e}_{q-1}\} \subset \mathbb{Z}^{q-1}$, then the tiling

$$\mathcal{T} = \{\mathbf{x} : 2 \mid x_{q-1} \text{ and } q \mid \mathbf{x} \cdot (1, 2, \dots, q-1); \\ \text{or } 2 \nmid x_{q-1} \text{ and } q \mid \mathbf{x} \cdot (q-1, \dots, 2, 1)\}$$

is not lattice.

First we show a rather surprising results that to prove this conjecture one can confine himself/herself to a specific tile. Later, to provide a supporting evidence, we show that the conjecture is true for all primes $q \leq 7$.

Theorem 22. Let q be a prime. If each tiling of \mathbb{Z}^{q-1} by the semi-cross $V_{q-1} = \{\mathbf{0}, \mathbf{e}_1, \dots, \mathbf{e}_{q-1}\}$ is lattice, then each tiling of \mathbb{Z}^n by a tile $V = \{\mathbf{0}, \mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$, where $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n , is a lattice tiling as well.

Proof. Let $\mathcal{T} = \{V+l, l \in \mathcal{L}\}$ be a tiling of \mathbb{Z}^n by a tile $V = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{q-1}\} \subset \mathbb{Z}^n$ of a prime size q such that $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n . We show that \mathcal{T} induces a tiling \mathcal{T}_0 of \mathbb{Z}^{q-1} by the semi-cross V_{q-1} .

Let $\phi : \mathbb{Z}^{q-1} \rightarrow \mathbb{Z}^n$ be a homomorphism defined by

$$(x_1, \dots, x_{q-1}) \mapsto \sum_{i=1}^{q-1} x_i \mathbf{v}_i.$$

Because of the condition that $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n , the homomorphism ϕ is surjective.

Let

$$\mathcal{T}_0 = \phi^{-1}(\mathcal{T}) = \left\{ (x_1, \dots, x_{q-1}) \in \mathbb{Z}^{q-1} : \sum_{i=1}^{q-1} x_i \mathbf{v}_i \in \mathcal{T} \right\}.$$

Since exactly one of $\mathbf{x}, \mathbf{x} + \mathbf{v}_1, \dots, \mathbf{x} + \mathbf{v}_{q-1}$ is contained in \mathcal{T} for each $\mathbf{x} \in \mathbb{Z}^n$, exactly one of $\mathbf{x}, \mathbf{x} + \mathbf{e}_1, \dots, \mathbf{x} + \mathbf{e}_{q-1}$ is contained in \mathcal{T}_0 for each $\mathbf{x} \in \mathbb{Z}^{q-1}$. Thus \mathcal{T}_0 is actually a tiling of \mathbb{Z}^{q-1} by $V_0 = \{\mathbf{0}, \mathbf{e}_1, \dots, \mathbf{e}_{q-1}\}$.

Because ϕ is surjective, the image is $\phi(\mathcal{T}_0) = \mathcal{T}$. If \mathcal{T}_0 is a subgroup of \mathbb{Z}^{q-1} , then \mathcal{T} also becomes a subgroup of \mathbb{Z}^n . Thus, it is sufficient to show that \mathcal{T}_0 is always a lattice tiling. \square

The following conjecture is equivalent to Conjecture 20.

Conjecture 23. Let $V = \{\mathbf{0}, \mathbf{v}_1, \dots, \mathbf{v}_{q-1}\} \subset \mathbb{Z}^n$ of a prime size q tiles \mathbb{Z}^n by translates, and $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n . Then there is a unique tiling, up to a congruency, of \mathbb{Z}^n by V and this tiling is lattice.

Indeed, if there were two non-congruent lattice tilings of \mathbb{Z}^n by V , then the induced tilings of \mathbb{Z}^{q-1} by semi-crosses would be non-congruent as well. However, by Theorem 18, all lattice tilings of \mathbb{Z}^{q-1} by semi-cross are congruent.

To provide supporting evidence we show that:

Theorem 24. *Let $V = \{0, v_1, \dots, v_{q-1}\}$ be a tile of a prime size $q \leq 7$ such that $\{v_1, \dots, v_{q-1}\}$ generate \mathbb{Z}^n . Then each tiling of \mathbb{Z}^n by V is lattice.*

To facilitate our discussion we introduce new notions and notation, and state several auxiliary results. Let $\mathcal{T} = \{V_{q-1} + l; l \in \mathcal{L}\}$ be a tiling of \mathbb{Z}^{q-1} by semi-crosses. We use terminology of coding theory; that is, the elements of \mathbb{Z}^{q-1} will be called words and the elements of \mathcal{L} , the centers of semi-crosses in \mathcal{T} , will be called codewords.

By a word of type $[m_1^{\alpha_1}, \dots, m_s^{\alpha_s}]$ we mean a word having α_1 coordinates equal to m_1 , \dots , α_s coordinates equal to m_s , the other coordinates equal to zero. Let W, Z be words, and the word $Z - W$ is of type $[m_1^{\alpha_1}, \dots, m_s^{\alpha_s}]$. Then Z will be called a word of type $[m_1^{\alpha_1}, \dots, m_s^{\alpha_s}]$ with respect to W . For $W = O$, we simplify the language and call Z shortly a word of type $[m_1^{\alpha_1}, \dots, m_s^{\alpha_s}]$. Further, we will say that a word V is covered by a codeword W if V belongs to the semi-cross centered at W . Finally, two words A, B coincide in t coordinates, if they have the same value in t non-zero coordinates.

The following theorem constitutes a crucial tool for proving the main result of this section.

Theorem 25. *Let \mathcal{T} be a tiling of \mathbb{Z}^{p-1} by semi-crosses. Then, for a prime p and any $k < p$, we have*

$$T\left(\sum_{i_1 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k}\right) = \frac{\binom{p-1}{k} - (-1)^k}{p} + (-1)^k T(1).$$

In other words, if O is a codeword then there are $\frac{1}{p}(\binom{p-1}{k} + (p-1)(-1)^k)$ codewords of type $[1^k]$, otherwise there are $\frac{1}{p}(\binom{p-1}{k} - (-1)^k)$ codewords of type $[1^k]$.

Proof. For convenience, we let

$$e_k = \sum_{i_1 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k}$$

denote the elementary symmetric polynomials. We use induction on k .

For $k = 1$ we get

$$\begin{aligned} T(e_1) &= T(x_1 + \dots + x_{q-1} + 1 - 1) = T(1 + x_1 + \dots + x_{q-1}) - T(1) \\ &= 1 - T(1) = \frac{\binom{p-1}{1} - (-1)^1}{p} + (-1)^1 T(1). \end{aligned}$$

Suppose now that the identity $T(e_j) = \frac{1}{p} \binom{p-1}{j} - (-1)^j + (-1)^j T(1)$ is true for all $1 \leq j < k$. Consider the identity

$$\left(\sum x_i^k \right) - e_1 \left(\sum x_i^{k-1} \right) + \cdots + (-1)^{k-1} e_{k-1} \left(\sum x_i \right) + (-1)^k k e_k = 0.$$

Note that it is true since all terms of the form $x_{i_1} \cdots x_{i_j} x_{i_{j+1}}^{k-j}$ are added and subtracted exactly once. It follows from this identity that

$$\begin{aligned} 0 &= T \left(\sum x_i^k \right) - T \left(e_1 \left(\sum x_i^{k-1} \right) \right) + \cdots + (-1)^k k T(e_k) \\ &= \sum_{j=0}^{k-1} (-1)^j T \left(e_j \left(\sum x_i^{k-j} \right) \right) + (-1)^k k T(e_k) \\ &= \sum_{j=0}^{k-1} (-1)^j \left[\binom{p-1}{j} - T(e_j) \right] + (-1)^k k T(e_k) \\ &= \sum_{j=0}^{k-1} \left[(-1)^j \left(\binom{p-1}{j} - \frac{1}{p} \binom{p-1}{j} \right) + \frac{1}{p} - T(1) \right] + (-1)^k k T(e_k) \\ &= \frac{p-1}{p} \sum_{j=0}^{k-1} (-1)^j \binom{p-1}{j} + k \left(\frac{1}{p} - T(1) \right) + (-1)^k k T(e_k) \\ &= \frac{p-1}{p} \sum_{j=0}^{k-1} (-1)^j \left(\binom{p-2}{j} + \binom{p-2}{j-1} \right) + k \left(\frac{1}{p} - T(1) + (-1)^k T(e_k) \right) \\ &= (-1)^{k-1} \frac{p-1}{p} \binom{p-2}{k-1} + k \left(\frac{1}{p} - T(1) + (-1)^k T(e_k) \right) \end{aligned}$$

since

$$\begin{aligned} T(e_j \left(\sum x_i^{k-j} \right)) &= T(e_j (1 + \sum x_i^{k-j})) - T(e_j) \\ &= e_j(1, \dots, 1) - T(e_j) = \binom{p-1}{j} - T(e_j). \end{aligned}$$

Hence we get

$$\begin{aligned} T(e_k) &= (-1)^{k+1} \left(\frac{1}{p} - T(1) \right) + \frac{p-1}{kp} \binom{p-2}{k-1} \\ &= \frac{1}{p} \left(\binom{p-1}{k} - (-1)^k \right) + (-1)^k T(1). \quad \square \end{aligned}$$

It is possible to prove a much more general statement than the above theorem; we skip the proof here as it is quite long and involved, and we do not need the statement in what follows.

Theorem 26. *Let \mathcal{T} be a tiling of \mathbb{Z}^{p-1} by semi-crosses, where p is a prime. Then, for any m_1, \dots, m_t and $\alpha_1, \dots, \alpha_t$, there are constants C and C' depending only on m_i 's and α_i 's such that the number of codewords of type $[m_1^{\alpha_1}, \dots, m_t^{\alpha_t}]$ is C if O is a codeword, otherwise it is C' .*

Now we state several corollaries of Theorem 25.

Corollary 27. *Let W be a codeword. Then there are $\frac{1}{p}(\binom{p-1}{k} + (p-1)(-1)^k)$ codewords of type $[1^k]$, and also of type $[-1^k]$ with respect to W .*

Proof. It suffices to consider the “shifted” tiling $\mathcal{T}_W = \{V_{q-1} + l, l \in \mathcal{L} - W\}$, and $\{V_{q-1} + l, l \in -\mathcal{L}\}$, a reflection of tiling \mathcal{T} . \square

Corollary 28. *For any $m, k \leq q-1$, the number of codewords of type $[m^k]$ with respect to W , equals the number of codewords of type $[1^k]$ with respect to W .*

Proof. It is sufficient to prove the statement only for $W = O$. To determine the number of codewords of type $[m^k]$ we need to calculate $T(e_k^{(m)})$, where $e_k^{(m)} = \sum_{i_1 < \dots < i_k} x_{i_1}^m x_{i_2}^m \dots x_{i_k}^m$. Thus, $e_k^{(1)} = e_k$ as defined above. It is not difficult to see that after substituting $y_i = x_i^m$ one can apply verbatim the proof of Theorem 25. \square

Substituting $k = q-1$, we get:

Corollary 29. *For each word W , W is a codeword if and only if $W \pm (1, 1, \dots, 1)$ is a codeword as well.*

Applying Corollary 12 we have

Corollary 30. *Let W be a codeword. Then, for any $a \leq q-1$, there is no codeword of type $[a^1]$ and of type $[a^1, -a^1]$ with respect to W .*

Finally,

Corollary 31. *Let W be a codeword. Then there are $n = \frac{q-1}{2}$ codewords U_1, \dots, U_n of type $[1^2]$, and $n = \frac{q-1}{2}$ codewords U'_1, \dots, U'_n of type $[-1^2]$ with respect to W . In addition,*

$$\sum_{i=1}^n U_i - W = I, \quad \sum_{i=1}^n U'_i - W = -I,$$

where $I = (1, 1, \dots, 1)$.

Proof. By Theorem 25, $n = \frac{q-1}{2}$. To see the other part of the statement it suffices to note that if two words $U_i - W$ and $U_j - W$ coincided in a coordinate then the semi-crosses centered at U_i and U_j would not be disjoint. \square

Proof of Theorem 24. By Theorem 22 it is sufficient to prove that each tiling of \mathbb{Z}^{q-1} by translates of $V = \{0, e_1, \dots, e_{q-1}\}$ is lattice. We start by introducing additional notation and notions. We denote by I the word $(1, 1, \dots, 1)$. For a word $W = (a_1, a_2, a_3, \dots, a_{q-1})$, by $\pi(W)$ we mean the word obtained by the shift of coordinates of W , i.e., $\pi(W) = (a_2, a_3, \dots, a_{q-1}, a_1)$; further we put $\langle W \rangle := \{W, \pi(W), \pi^2(W), \dots, \pi^{q-2}(W)\}$, the set of all shifts of W .

$q = 2$. Trivially, each tiling of \mathbb{Z}^1 by the tile $V_1 = \{0, e_1\}$ is lattice.

$q = 3$. By Corollary 29, for all integers n , nI is a codeword, and from periodicity of \mathcal{L} , if W is a codeword then $W + 3ne_1$ is a codeword as well. Thus, \mathcal{L} contains a lattice F generated by I and $3e_1$. However, $F = \mathcal{L}$ as

$$\det \begin{vmatrix} 1 & 1 \\ 3 & 0 \end{vmatrix} = -3.$$

In what follows, there will be several statements formulated for a general codeword W but we will prove them all without loss of generality only for $W = O$. Further, we point out, that with respect to a cyclic property, it suffices to prove statements given below only for one codeword from a set $\langle V \rangle$.

$q = 5$. Let W be a codeword. By Corollary 31, there are two codewords A, B of type $[1^2]$, $A + B = I$, and two codewords C, D of type $[-1^2]$, $C + D = -I$, with respect to W ; we denote them by $\mathcal{U}_2^+(W)$ and $\mathcal{U}_2^-(W)$, respectively. To simplify the proof, we assume without loss of generality that $\mathcal{U}_2^+(O) = \langle (1, 0, 1, 0) \rangle$. There are 6 words of type $[1^2]$, each of them covered by a codeword either of type $[1^2]$ or of type $[1^2, -1]$. Hence, as there are 2 codewords of type $[1^2]$, there have to be 4 codewords of type $[1^2, -1]$, we denote them by $\mathcal{U}_3^+(W)$; the same is true for codewords of type $[-1^2, 1]$, they will be denoted $\mathcal{U}_3^-(W)$. The following straightforward claim will be applied repeatedly in the proof.

Claim 1. Each codeword in $\mathcal{U}_2^+(W)$ determines uniquely the other codeword in $\mathcal{U}_2^+(W)$. In addition, codewords in $\mathcal{U}_2^+(W)$, and one codeword in $\mathcal{U}_3^+(W)$, determine uniquely the other codewords in $\mathcal{U}_3^+(W)$. The same is true for the “ $-$ ” part.

For example, if $\mathcal{U}_2^+(O) = \langle (1, 0, 1, 0) \rangle$, then we have $\mathcal{U}_3^+(O) = \langle (1, 1, -1, 0) \rangle$ or $\mathcal{U}_3^+(O) = \langle (1, 1, 0, -1) \rangle$. Thus, one codeword in $\mathcal{U}_3^+(O)$ determines in a unique way the set $\mathcal{U}_3^+(O)$.

Claim 2. Let W be a codeword. Then, for each $A \in \mathcal{U}_2^+(W)$,

$$\mathcal{U}_2^+(W + A) = \mathcal{U}_2^+(W).$$

Proof of Claim 2. Let $W = O$ without loss of generality. As I is a codeword, it means that $(0, 1, 0, 1) \in \mathcal{U}_2^+((1, 0, 1, 0))$, and therefore $\mathcal{U}_2^+((1, 0, 1, 0)) = \mathcal{U}_2^+(O)$. Further, since $\langle (1, 0, 1, 0) \rangle - I = -\langle (1, 0, 1, 0) \rangle$ are codewords, we get

$$\mathcal{U}_2^-(O) = -\mathcal{U}_2^+(O),$$

which implies

$$\mathcal{U}_2^-(W + A) = \mathcal{U}_2^-(W), \text{ for any codeword } A \in \mathcal{U}_2^-(W).$$

It follows that $\mathcal{U}_2^+(W + A) = \mathcal{U}_2^-(W)$. □

Then, by a straightforward induction, tiling \mathcal{T} contains a lattice generated by $\langle(1, 0, 1, 0)\rangle$. Now we will show that \mathcal{T} contains a lattice generated by $\langle(1, 0, 1, 0)\rangle$ and any codeword in $\mathcal{U}_3^+(O)$.

Claim 3. $\mathcal{U}_3^-(O) = -\mathcal{U}_3^+(O)$.

Proof of Claim 3. Assume by contradiction that $\mathcal{U}_3^-(O) \neq -\mathcal{U}_3^+(O)$, say without loss of generality, $\mathcal{U}_3^+(O) = \langle(1, 1, -1, 0)\rangle$, and $\mathcal{U}_3^-(O) = -\langle(1, 1, 0, -1)\rangle$. Then, $U = (1, 1, -1, 0) \in \mathcal{U}_3^+(O)$, and $V = (1, -1, -1, 0) \in \mathcal{U}_3^-(O)$. However, this contradicts Corollary 30 as $U - V$ is of type $[2^1]$. \square

Claim 4. For any $A \in \mathcal{U}_2^+(W)$,

$$\mathcal{U}_3^+(W + A) = \mathcal{U}_3^+(W),$$

and, for any $A \in \mathcal{U}_3^+(W)$,

$$\mathcal{U}_2^+(W + A) = \mathcal{U}_2^+(W).$$

Proof of Claim 4. Let $W = O$. Assume without loss of generality that $\mathcal{U}_3^+(O) = \langle(1, 1, -1, 0)\rangle$. It is sufficient to notice that $B + C - I$ is a codeword for each $B \in \langle(1, 0, 1, 0)\rangle$, and $C \in \langle(1, 1, -1, 0)\rangle$. \square

In view of Claim 3, Claim 4 is true also for the “ $-$ ” part.

Claim 5. Let $\mathcal{U}_2^+(W) = \langle(1, 0, 1, 0)\rangle$. Then $\mathcal{U}_3^+(W + A) = \mathcal{U}_3^+(W)$ for any $A \in \mathcal{U}_3^+(W)$.

Proof of Claim 5. Assume that $\mathcal{U}_3^+(A) \neq \mathcal{U}_3^+(O)$ for an $A \in \mathcal{U}_3^+(O)$, say without loss of generality that $\mathcal{U}_3^+(O) = \langle(1, 1, -1, 0)\rangle$, and $\mathcal{U}_3^+((1, 1, -1, 0)) = \langle(1, 1, 0, -1)\rangle$. Then $(1, 1, -1, 0) + (0, -1, 1, 1) = (1, 0, 0, 1)$ would be a codeword, a contradiction since $\mathcal{U}_2^+(W) = \langle(1, 0, 1, 0)\rangle$. \square

As above, by Claim 3, Claim 5 is true also for the “ $-$ ” part. Assume without loss of generality that $\langle(1, 1, -1, 0)\rangle$ are codewords. Let n, m, k be integers. By Claim 2, $W = n(1, 0, 1, 0) + m(0, 1, 0, 1)$ is a codeword, and $\mathcal{U}_2^\pm(W) = \pm\langle(1, 0, 1, 0)\rangle$. By Claim 4 and Claim 5, and a straightforward induction, $W + k(1, 1, -1, 0)$ is a codeword. Finally, taking into account that \mathcal{T} is periodic with $5e_1$, we have that \mathcal{T} contains a lattice \mathcal{R} generated by $\langle(1, 0, 1, 0)\rangle$, $(1, 1, -1, 0)$, and $5e_1$. The determinant of the matrix whose rows are the given four vectors equals ± 5 , thus \mathcal{R} contains all codewords of \mathcal{T} . The proof for $q = 5$ is complete.

$q = 7$. By Theorem 25, for each codeword W there are 3 codewords of type $[1^2]$ and 2 codewords of type $[1^3]$ with respect to W ; we denote these codewords by $\mathcal{U}_2(W)$ and $\mathcal{U}_3(W)$, respectively.

Lemma 32. *Let W be a codeword. Then*

$$\sum_{V \in \mathcal{U}_2(W)} V = \sum_{Z \in \mathcal{U}_3(W)} Z = (1, 1, 1, 1, 1, 1).$$

Proof of Lemma. Let $W = O$. The statement is obvious for $\mathcal{U}_2(W)$. To show it for $\mathcal{U}_3(W)$, we need in fact to prove that the two codewords Z_1 and Z_2 of type $[1^3]$ do not coincide in any coordinate. Z_1 and Z_2 cannot coincide in two coordinates, otherwise the two semi-crosses centered at Z_1 and Z_2 would have a non-empty intersection. So assume by contradiction that Z_1 and Z_2 coincide in exactly one coordinate. Let, without loss of generality, $Z_1 = (1, 0, 1, 0, 1, 0)$ and $Z_2 = (1, 0, 0, 1, 0, 1)$. Now we show that

Claim 6. For each codeword W there are

- (i) 3 codewords of type $[1^4]$; for each $1 \leq i \leq 6$, exactly one of the three codewords has the i -th coordinate equal to 0;
- (ii) 6 codewords of type $[1^4, -1^1]$ with respect to W . No two of these codewords coincide in the coordinate whose value is -1 .

Proof of Claim 6. Let $W = O$.

- (i) There is no codeword of type $[1^5]$. So all 6 words of this type are covered by the codewords of type $[1^4]$, the statement follows.
- (ii) There are 15 words of type $[1^4]$; 3 of them are codewords, 6 of them are covered by codewords of type $[1^3]$ (regardless of in how many coordinates Z_1 and Z_2 might coincide). Thus the remaining 6 words have to be covered by codewords of type $[1^4, -1^1]$. Clearly, each codeword of type $[1^4, -1^1]$ covers only one word of type $[1^4]$, thus there are 6 codewords of type $[1^4, -1^1]$. Two semi-crosses centered at codewords of type $[1^4, -1^1]$ coinciding in the coordinate whose value is -1 would have a non-empty intersection. \square

Now we are ready to finish the proof of our lemma. Let Z be a codeword of type $[1^4]$ whose second coordinate equals 0. The three codewords Z , Z_1 , and Z_2 cover all 5 words of type $[1^4]$ whose second coordinate equals to 0. However, by Claim 6, there is a codeword W of type $[1^4, -1^1]$ whose second coordinate equals -1 . Clearly, W also covers a word of type $[1^4]$ whose second coordinate is 0, a contradiction. The proof is complete. \square

We note that any codeword of type $[1^3]$ coincides with each codeword of type $[1^2]$ in precisely one coordinate. We will assume without loss of generality that $\mathcal{U}_2(O) = \langle (1, 0, 0, 1, 0, 0) \rangle$, and $\mathcal{U}_3(O) = \langle (1, 0, 1, 0, 1, 0) \rangle$. Also we set, $B_1 = (1, 0, 0, 1, 0, 0)$, and $B_2 = \pi(B_1)$, $B_3 = \pi^2(B_2)$.

Claim 7. Let W be a codeword. Then $\mathcal{U}_2(W + A) = \mathcal{U}_2(W)$ for all $A \in \mathcal{U}_2(W)$. In particular, the 3 codewords of type $[1^4]$ are $\langle (0, 1, 1, 0, 1, 1) \rangle$, and the 3 codewords of type $[2^2]$ are $2 \cdot \mathcal{U}_2(O) = \langle (2, 0, 0, 2, 0, 0) \rangle$. Further, tiling \mathcal{T} contains a lattice generated by codewords $\langle (1, 0, 0, 1, 0, 0) \rangle$.

Proof of Claim 7. Let $W = O$. To prove the statement it suffices to show that the 3 codewords of type $[1^4]$ are $\langle(0, 1, 1, 0, 1, 1)\rangle$.

By Corollary 28, there are 3 codewords of type $[2^2]$. We show that these codewords are $2 \cdot \langle(1, 0, 0, 1, 0, 0)\rangle = \langle(2, 0, 0, 2, 0, 0)\rangle$. Assume that there is codeword W of type $[2^2]$ such that $W \notin \langle(2, 0, 0, 2, 0, 0)\rangle$. Let V be a codeword of type $[1^2, -1]$ such that V and $\frac{1}{2}W$ coincide in two coordinates. Then $W - V = Z$ is of type $[1^3]$. Hence, $Z \in \mathcal{U}_3(V)$, and $Z' = I - Z \in \mathcal{U}_3(V)$ as well. Thus, $V + Z'$ is a codeword, and it is of type $[1^5, -1]$. This is a contradiction as I is a codeword. Therefore, $B_i \in \mathcal{U}_2(B_i)$, $i = 1, 2, 3$. Let C_2, C_3 be the other two codewords in $\mathcal{U}_2(B_1)$. Then $C_2 + C_3 = (0, 1, 1, 0, 1, 1)$ and $B_1 + C_i$, $i = 2, 3$, are codewords of type $[1^4]$. By Claim 6, $(0, 1, 1, 0, 1, 1)$ has to be a codeword. However, this means that $B_2 \in \mathcal{U}_2(B_3)$, and therefore also $B_1 \in \mathcal{U}_2(B_3)$; that is, $\mathcal{U}_2(B_3) = \mathcal{U}_2(O)$. By the same argument we get $\mathcal{U}_2(B_i) = \mathcal{U}_2(O)$ for $i = 2, 3$. But then $(1, 1, 0, 0, 1, 1)$ is a codeword, a contradiction. The proof of the first part is complete. Clearly, as $\mathcal{U}_2(B_1) = \mathcal{U}_2(O)$, $\langle(1, 1, 0, 1, 1, 0)\rangle$ are the three codewords of type $[1^4]$. The final part of the proof follows by a straightforward induction. \square

Let $\mathcal{U}_2(W) = \langle(1, 0, 0, 1, 0, 0)\rangle$, and $\mathcal{U}_3(W) = \langle(1, 0, 1, 0, 1, 0)\rangle$. Then the three codewords of type $[1^4]$ are $\langle(1, 1, 0, 1, 1, 0)\rangle$. Further, the 6 codewords of type $[1^4, -1]$ with respect to W are either $\langle(1, 1, 1, 1, -1, 0)\rangle$, or $\langle(1, 1, 1, 1, 0, -1)\rangle$. We denote these codewords by $\mathcal{U}_4(W)$.

Claim 8. Let W be a codeword, $\mathcal{U}_2(W) = \langle(1, 0, 0, 1, 0, 0)\rangle$, and $\mathcal{U}_3(W) = \langle(1, 0, 1, 0, 1, 0)\rangle$. If $\mathcal{U}_4(W) = \langle(1, 1, 1, 1, -1, 0)\rangle$, then the 6 codewords of type $[1^3, -1]$ are $\langle(1, 1, 1, 0, 0, -1)\rangle$, and the 12 codewords of type $[1^2, -1^1]$ are $\langle(1, 1, 0, -1, 0, 0)\rangle$, and $\langle(1, -1, 1, 0, 0, 0)\rangle$. If $\mathcal{U}_4(W) = \langle(1, 1, 1, 1, 0, -1)\rangle$, then the 6 codewords of type $[1^3, -1]$ are $\langle(1, 1, 1, -1, 0, 0)\rangle$, and the 12 codewords of type $[1^2, -1^1]$ are $\langle(1, 1, 0, 0, -1, 0)\rangle$, and $\langle(1, -1, 1, 0, 0, 0)\rangle$.

Proof of Claim 8. Let $W = O$. The six words of type $[1^4]$ that are covered by codewords of type $[1^4, -1]$ are $\langle(1, 1, 1, 1, 0, 0)\rangle$. By Claim 6, the codewords of type $[1^4, -1]$ are either $\langle(1, 1, 1, 1, -1, 0)\rangle$ or $\langle(1, 1, 1, 1, 0, -1)\rangle$. Assume the former case. The six words of type $[1^3]$ that are covered by codewords of type $[1^3, -1]$ are $\langle(1, 1, 1, 0, 0, 0)\rangle$. Thus, the codewords of type $[1^3, -1]$ have to be $\langle(1, 1, 1, 0, 0, -1)\rangle$, otherwise the semi-crosses centered at $\langle(1, 1, 1, 1, -1, 0)\rangle$ and at codewords of type $[1^3, -1]$ would not be disjoint. Finally, the 12 words of type $[1^2]$ covered by codewords of type $[1^2, -1]$ are $\langle(1, 1, 0, 0, 0, 0)\rangle$ and $\langle(1, 0, 1, 0, 0, 0)\rangle$. Because of codewords $\langle(1, 1, 1, 0, 0, -1)\rangle$, the codewords covering words $\langle(1, 1, 0, 0, 0, 0)\rangle$ and $\langle(1, 0, 1, 0, 0, 0)\rangle$ are the codewords $\langle(1, 1, x, y, 0, 0)\rangle$ and $\langle(1, z, 1, v, w, 0)\rangle$, where one of x, y is -1 and the other equals 0, also one of z, v, w equals -1 , the other two are 0's. With respect to $(1, 0, 1, 0, 1, 0)$, it is $w = 0$. If $x = -1$, then semi-crosses $\langle(1, 1, x, y, 0, 0)\rangle$ and $\langle(1, z, 1, v, 0, 0)\rangle$ would intersect. For the same reason it is impossible to have $y = v = -1$. Using the same ideas one can show the other part of the claim for the latter case. \square

Claim 9. If W is a codeword described in Claim 8, then $-W$ is a codeword as well.

Proof of Claim 9. We know that if W is a codeword then $W \pm I$ is also a codeword. Hence,

$$\langle(1, 1, 0, 1, 1, 0)\rangle - I = -\langle(1, 0, 0, 1, 0, 0)\rangle = -\mathcal{U}_2(W)$$

are codewords. Further,

$$\mathcal{U}_3(W) - I = -\langle(1, 0, 1, 0, 1, 0)\rangle = -\mathcal{U}_3(W)$$

are codewords as well. Applying Claim 8 to $-\mathcal{U}_2(W)$ and $-\mathcal{U}_3(W)$ we need only to show that if $\langle(1, 1, 1, 1, -1, 0)\rangle$ ($\langle(1, 1, 1, 1, 0, -1)\rangle$) are codewords, then $-\langle(1, 1, 1, 1, -1, 0)\rangle$, ($-\langle(1, 1, 1, 1, 0, -1)\rangle$) are again codewords. Assume by contradiction that $\langle(1, 1, 1, 1, -1, 0)\rangle$ and $-\langle(1, 1, 1, 1, 0, -1)\rangle$ are codewords. Then, by Claim 8, $\langle(1, 1, 1, 0, 0, -1)\rangle$ and $\langle(-1, -1, -1, 1, 0, 0)\rangle$ are codewords as well. Set $Z = (1, 1, 1, 0, 0, -1)$, and $U = (-1, -1, 1, 0, 0, -1)$. Then $Z - U = (2, 2, 0, 0, 0, 0)$ is a codeword of type $[2^2]$ with respect to U . This in turn implies, see Claim 7, that $(1, 1, 0, 0, 0, 0)$ is a codeword of type $[1^2]$ with respect to U , that is, $U + (1, 1, 0, 0, 0, 0) = (0, 0, 1, 0, 0, -1)$ is a codeword. However, this contradicts Corollary 29. The proof is complete. \square

Claim 10. $\mathcal{U}_3(W + B) = \mathcal{U}_3(W)$ for all $B \in \mathcal{U}_2(W)$, and $\mathcal{U}_2(W + B) = \mathcal{U}_2(W)$ for all $B \in \mathcal{U}_3(W)$.

Proof of Claim 10. Let $W = O$. It suffices to note that for each $U \in \langle(1, 0, 1, 0, 1, 0)\rangle$, and each $Z \in \langle(1, 0, 0, 1, 0, 0)\rangle$, $U + Z - I$ is a codeword. \square

Claim 11. $\mathcal{U}_3(W + B) = \mathcal{U}_3(W)$ for all $B \in \mathcal{U}_3(W)$.

Proof of Claim 11. Let $W = O$. Assume by contradiction that $\mathcal{U}_3(B) \neq \mathcal{U}_3(O)$. Then there is C in $\mathcal{U}_3(B)$ such that $B_4 = (1, 0, 1, 0, 1, 0)$ coincides with C only in one coordinate. This in turn implies that $B_4 + C - I$ is of type $[1, -1]$, a contradiction. \square

By Claim 8, 10, and 11 we have that the tiling \mathcal{T} contains a lattice generated by $\langle(1, 0, 0, 1, 0, 0)\rangle$ and $(1, 0, 1, 0, 1, 0)$.

Claim 12. Let W be a codeword. Then $\mathcal{U}_2(W + B) = \mathcal{U}_2(W)$, $\mathcal{U}_3(W + B) = \mathcal{U}_3(W)$, and $\mathcal{U}_4(W + B) = \mathcal{U}_4(W)$ for all $B \in \mathcal{U}_4(W)$.

Proof of Claim 12. As this proof uses the same techniques as presented above we leave it for the reader. \square

With Claim 12 in hands we know that \mathcal{T} contains a lattice generated by $\langle (1, 0, 0, 1, 0, 0) \rangle, (1, 0, 1, 0, 1, 0)$, and a vector from $\mathcal{U}_4(W)$, say either $(1, 1, 1, 1, -1, 0)$ or $(1, 1, 1, 1, 0, -1)$. In addition, \mathcal{T} is periodic with $7e_1$. The determinant of a matrix whose rows are these 7 vectors is ± 7 ; that is, the lattice contains all codewords of \mathcal{T} . \square

As an immediate consequence of Theorem 18 we get:

Corollary 33. *let $V = \{0, \mathbf{v}_1, \dots, \mathbf{v}_{q-1}\} \subset \mathbb{Z}^n$ of a prime size $q \leq 7$ tiles \mathbb{Z}^n by translates, and $\{\mathbf{v}_1, \dots, \mathbf{v}_{q-1}\}$ generate \mathbb{Z}^n . Then there is a unique tiling, up to a congruency, of \mathbb{Z}^n by V and this tiling is lattice. In particular, for a prime $q \leq 7$, there is a unique tiling, up to a congruency, of \mathbb{Z}^{q-1} by semi-crosses.*

Remark 34. *We note that a computer aided proof that there is only one tiling of \mathbb{Z}^4 by semi-crosses is provided in [13] without relating the result to other tiles of size 5.*

We note that in the proof of the above theorem we have not used explicitly the fact that q is a prime. We believe that the property distinguishing tilings by semi-crosses of prime size from tilings by semi-crosses of composite size is that of being cyclic. We recall that a tiling $\mathcal{T} = \{V + l; l \in \mathcal{L}\}$ is called cyclic if, for each codeword l ,

$$l \in \mathcal{L} \Rightarrow \langle l \rangle \subset \mathcal{L} ;$$

that is, if for any codeword, also all its shifts are codewords. In this regard, at

the very end of the paper we show that:

Claim 35. *For each prime $q > 2$, there is a cyclic tiling of \mathbb{Z}^{q-1} by semi-crosses.*

Proof. For a primitive element t of the multiplicative group \mathbb{Z}_q^* we define a homomorphism $\phi : \mathbb{Z}^{q-1} \rightarrow \mathbb{Z}_q$ by

$$\phi(e_i) = t^{i-1} \text{ for } i = 1, \dots, q-1.$$

Then $\mathcal{T} = \{V_{q-1} + l; l \in \mathcal{L} = \ker(\phi)\}$ is a lattice tiling of \mathbb{Z}^{q-1} by semi-crosses. Let $a = (a_1, \dots, a_{q-1}) \in \mathcal{L}$. Then

$$a_1 t^0 + a_2 t^1 + \dots + a_{q-1} t^{q-2} \equiv 0 \pmod{q}$$

Multiplying the congruence by t^k yields

$$a_1 t^{0+k} + a_2 t^{1+k} + \dots + a_{q-1} t^{q-2+k} \equiv 0 \pmod{q};$$

that is $\pi^k(a)$, the shift of a by k to the right, is a codeword as well. \square

References

- [1] D. Beauquier, M. Nivat, *On translating one polyomino to tile the plane*, Discrete & Computational Geometry 6(1991), 575-592.
- [2] S. W. Golomb, L. R. Welsh, *Perfect codes in the Lee metric and the packing of polyominoes*, SIAM J. Applied Math. 18(1970), 302-317.
- [3] G. Hajós, *Über einfache und mehrfache Bedeckung des n -dimensional Raumes mit einem Würfelgitter*, Math. Zeitschr. 47(1942), 427-467.
- [4] D. Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. 42(1890), 313-373.
- [5] P. Horak, B. AlBdaiwi, *Non-periodic tilings of \mathbb{R}^n by crosses*, Discrete & Computational Geometry 47(2012), 1-16.
- [6] P. Horak, B. AlBdaiwi, *Diameter perfect Lee codes*, IEEE Trans. on Information Theory 58(2012), 5490-5499.
- [7] P. Horak, V. Hromada, *Tiling \mathbb{R}^5 by crosses*, Discrete & Computational Geometry 51(2014), 269-284.
- [8] J. Kari, M. Szabados, *An algebraic approach to Nivat's conjecture*, arXiv:1510.001771v1, Oct 1, 2015.
- [9] O.H. Keller, *Über die lückenlose Einföllung des Raumes mit Würfeln*, J. Reine Angew. Math 177(1930), 231-248.
- [10] J. C. Lagarias, Y. Wang, *Tiling the line with translates of one tile*, Inventiones Mathematicae 124(1996), 341-365.
- [11] H. Minkowski, *Dichtestegittenformige Lagerung kongruenter Körper*, Nachrichten Ges. Wiss. Gottingen (1904), 311-355.
- [12] M. Nivat, Invited talk at ICALP, Bologna, 1997.
- [13] S. Szabo, *Low dimensional tilings by certain crosses and semi-crosses*, Symmetry: Culture and Science 21(2010), 333-343.
- [14] M. Szegedy, *Algorithms to tile the infinite grid with finite clusters*, FOCS, IEEE Computer Society (1998), 137-147.